The Secure Conferencing User Agent
A Tool to Provide Secure Conferencing with MBONE
Multimedia Conferencing Applications

Elfriede Hinsch, Anne Jaegemann, Ian C. Roper, Lan Wang

Abstract: This report briefly describes the Secure Conferencing User Agent (SCUA), which provides secure conferencing with privacy and authentication. The SCUA was implemented using the MICE multimedia conferencing applications with built-in encryption and the security infrastructure developed in the Password Project. Both MICE and Password were projects of the European Union. The paper describes the first prototype of the SCUA which was developed by GMD in the MICE project and the planned enhancements of it.

Content
1 The MICE Project
2 Motivation
3 Conferencing Technology
4 Security Technology
5 The Secure Conferencing User Agent
6 Description of a Secure Conference
7 Experience and Further Works

1 The MICE Project

MICE (‘Multimedia Integrated Conferencing for European Researchers’) [1] was an Esprit Project of the European Union with the objective of providing for European scientists means and ways for multimedia conferencing.

The project started as a one year project in December 1992 and was subsequently extended until September 95. The security work was started July 94.

Partners of the project were: University College of London UCL (UK), project leader, GMD Darmstadt (Germany), INRIA (France), Telenor (Norway), Oslo University (Norway), Rechenzentrum der Universitaet Stuttgart (Germany), Swedish Institute for Computer Science (Sweden), and Universite Libre de Bruxelles (Belgium).
2 Motivation

One characteristic of the present MICE technology is its openness. Once someone has started a conference anyone who gets to know of the used addresses and port numbers can participate. Since the conference tools make use of the Internet Mbone broadcast facilities, there is no support by the system to prevent other (unauthorized) users from taking part in a conference.

Some applications may require that a conference be restricted to a determinable closed user-group. Users outside such a user-group must not be able to take part. Examples are (tele-)seminars where only those who have paid the fee for it can participate or (tele-)meetings which are restricted to the members of a project. Such applications need some kind of access control to prevent unauthorized users from taking part in the conference. Other applications may require in addition, that the information exchanged among the partners be kept confidential.

3 The Conferencing Technology

The basic philosophy for MICE multimedia conferencing was to make good use of available equipment and tools and to require as little as possible in addition to general purpose workstations and data networks. Participating in MICE conferences is possible from either a single workstation or a conference room. A workstation is usually found on an individual's desktop. For the purpose of MICE, it has to be equipped with video camera, microphone, loudspeaker, and appropriate conferencing software.

![Multimedia Workstation performing video coding and decoding in software](image)

The infrastructure for the data transport is based on packet switched networks with Internet protocols and on the Mbone as a virtual network [2], which allows applications to work in a multicast mode (one-to-many connections) without the need for any central service. Among the software tools used in MICE are the following: SD is a tool for creating, announcing and joining a conference [5], VAT is the conference tool used for audio [3], WB is a whiteboard which substitutes for a regular whiteboard as well as a